General MiTS communication system

Failure Mode, Effect and Criticality Analysis

FMECA

V 1.0

Contents:

Abbreviations:

MiTS	-	Maritim IT Standard
MNS	-	MiTS Network Station
MAU	-	MiTS Application Unit
MAPI	-	MiTS Application Interface
LNA	-	Local Network Administrator
CNA	-	Communication Node for Administrative messages
NWI	-	NetWork Interface
UPS	-	Uninterruptible Power Supply
RAM	-	Random Access Memory
EMI	-	ElecroMagnetic Interference
PCB	-	Printed Circuit Board

1. Introduction

1.1. Scope of work

The study should be performed in order to identify failure modes which might cause reduced or loss of communication functions.

The method to be used for the analysis should be Failure Mode, Effect and Criticality Analysis (FMECA). The FMECA is a general qualitative analysis, including a ranking of probability occurrence and severity of consequence (criticality). The failure cause is also included, primarily to give information on the reason for including the failure mode.

Counteractions should be suggested if and when deemed necessary in order to increase the availability and reliability.

The areas to be covered by the analysis are the general communication mechanisms offered in MiTS including necessary hardware and includes the following:

- Inter-node communication (software)
- Hardware, including cables and cable connectors
- Redundant network

under the following operation condition

- Start-up and initialisation
- Normal operation
- High load condition

For redundant network, the analysis covers a solution using two network cards for each node and no additional hardware between the nodes.

1.2. Study boundaries and assumptions

The areas not covered by the analysis are the following:

- Operator interface
- Applications

The following environmental and general conditions have been assumed:

- Ambient temperature: +5 to +55°C
- Humidity: 96 % R.H.
- Vibrations: 2-100 Hz, Amplitude ±1 mm/sec below 13.2 Hz and 0.7 g above 13.2 Hz.
- Electric supply: Typically 230 V +10% to - 15%, 50 Hz ±5%, 24 VDC +25% to -35%

It is further assumed that :

- The components selected are of marine or industrial standard types or having a reliability equivalent to or even better than these.
- The servicing and maintenance of the installation is according to stated procedures, and that defective parts are repaired or replaced without undue delay. (It has not been assumed that parts are replaced before failing i.e. predictive maintenance).
- The systems are operated by competent personnel.

1.3. Work procedure

The basis for the study is the general MiTS documentation. The system has been broken down by DNVC into components, e.g. hardware parts and complete software tasks. The lowest level at which the analysis is effective is the level for which information was available to establish definition and description of functions, or down to the lowest level of replaceable elements. The system break-down structure as described below was selected to be able to separate and analyse each function:

- Logic failure effect block diagrams have been established. The diagrams, which are comparable to failure trees, describe all components and systems which have to be operative for the function to work.

- A list of failure modes for the different components was established for each operational phase by introduction of potential failure modes component by component.

- A FMECA was then carried out by SINTEF. A number of potential failures which may have significant effect on the operation have been identified and commented.

- Suggested remedies to overcome the effects or reduce the possibility for such failures to occur have been given by SINTEF.

1.4. Failure modes

At the lowest level, the basic failure modes that were applied for each element, can be described as follows:

- Loss of output, loss of function
- Maloperation, output deviates from the specification but the component is still operating.
- Inadvertent operation, erroneous output signal e.g. communication without request, premature signal.
- Structural failure, breakdown, crack, rupture, leak.

The following basic causes for failures were applied:

- Malfunction, incorrectly output due to an internal failure
- Maloperation, an operation not according to plans
- Erroneous input, an external cause of failure
- Parameters exceeded, unforeseen conditions
- Design deficiency, the quality is not according to the specification or project requirements
- Wear & tear, lack of maintenance

1.5. Comments to results

The comments given have been grouped in the following way:

a) <u>Critical findings (CF)</u>

The comments categorised as ’critical findings’ concern items or functions identified as design features which might cause reduced or loss of functions in a critical manner i.e. by combination of probability and consequence appearing as unacceptable.

b) <u>Engineering comments (EC)</u>

The comments categorised as ’engineering comments’ concern items or functions identified as design features to be modified in order to improve system performance, reliability, operation safety and/or deemed as a better solution from an engineering point of view.

c) Items requiring further investigations (FI)

Items categorised as 'items requiring further investigation' are design features identified as inadequately documented, beyond the scope of our FMECA and/or areas regarded as a matter of concern to be brought to attention.

1.6. Table description

Case	-	Reference number
Operation	-	Operational phase (Start-up, Normal operation and High load condition.
Component	-	See 1.7.
Failure mode	-	See 1.5.
Possible failure cause	-	Indicating possible causes for each failure mode. The column is not strictly part of the analysis, but is included for convenience.
Detection	-	How the failure is detected by the system.
Local effect	-	Effect of the failure for the component and within the node.
Overall effect	-	Effect on the rest of the system. Information on how the communication function is influenced is to be included.
Prob.	-	Probability of entering the failure mode according to table 2.1.1.
Cons.	-	Consequence of the failure according to table 2.1.2.
Remark	-	Additional information not relevant for the previous columns.

1.7. System description

A minimum network arrangement is as shown in Figure 1.4 below.

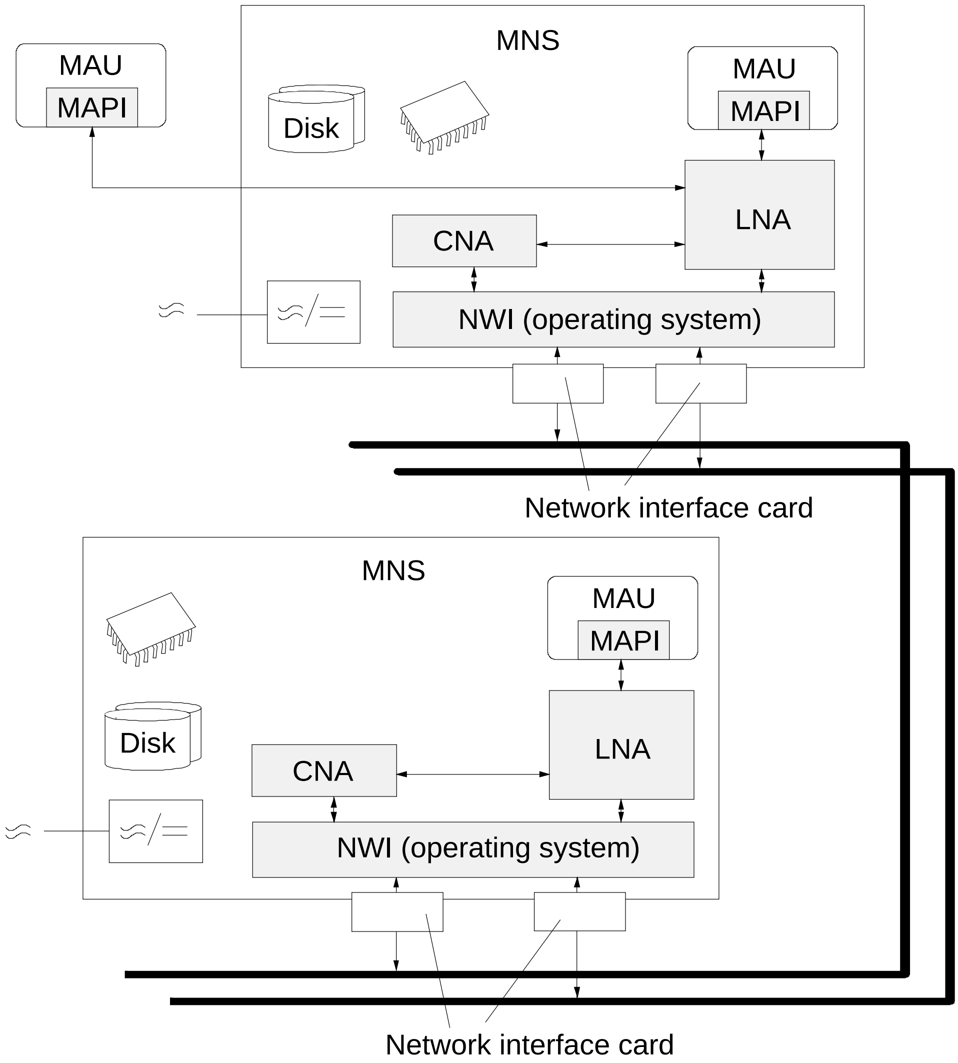

Figure 1.4 MiTS general network

Main components of the network:

Component	No.
Power supply	1 per node
Disk(s)	1 to n per node
RAM	n Mbyte per node
NWI (part of operating system)	1 per node
CNA	1 per node
LNA	1 per node
MAU incl. MAPI	1 to n per node
Serial lines	zero to n per node
Network interface card	1 (2) per node [1)]
Network cable(s) with connectors	1 (2) [1)]

[1)] 2 for redundant network.

Table 1.4.1. Network components

2. Failure Mode, Effect and Criticality Analysis

2.1. General

2.1.1 Component and system reliability

In order to differentiate between probabilities of occurrence, relevant failure rates have been used. For systems constituted by several interlinked components, the sum of failure rates of each individual has been applied. ($\lambda = \Sigma\lambda_i$). In cases were reliability data has not been available, the probability of occurrence has been given to our best engineering judgement.

The applied failure rates are simplified such that they are derived by assuming that the components are in continuous operation until they fail.

Probability	**Failure rate**	**Remarks**
High	< 1 year	Frequent
Medium	< 10 year	Reasonably probable
Low	< 100 year	Remote
Low-low	> 100 years	Rare

Table 2.1.1 Probabilities

The probabilities found in Table 2.1.1 applies to hardware only. For software, the failure rate for the different probabilities are normally higher. No exact figures are suggested in this analysis. The main difference between hardware and software is that a failure in the hardware is not self-correcting, whereas software failures may be corrected by automatic restart of computer tasks.

2.1.2 Definition of consequences

In order to differentiate between the categories of consequences, the severity classes listed below have been used. Note that economical consequences, injury to personnel, pollution or economical impacts have not been considered.

Category	**Effect on system**	**Loss of function**	**Remarks**	
Critical	Total system dead-lock	All communication	Unacceptabl e	Unsafe
Severe	Invalid transactions, excess latency	Normal operation (several nodes)	To be avoided	
Marginal	Disturbance	Functions belonging to one node	Unscheduled repair	Relatively safe
Safe	Insignificant	Sub-system or component (MAU)	Failure easily mandible	

Table 2.1.2 Consequences

2.1.3 Common cause failures

Is assumed that power supplies to each node is separately fused, and the only common failure for power is at black-out. By using a UPS for each node, this common cause failure will be eliminated.

As for the network cabling including its connectors, this will be a common mode for a single network. For redundant network, it is assumed that the cabling is physically separated as far as possible to avoid any common failure for any single external event such as local fire and flooding. To avoid this situation, the cabling must not be routed via common locations. This may be arranged by use of drop cables where the transducers handles a short circuit in the drop cable without short-circuiting the network cable, by use of segmetations of the network, or by use of a start network handling short circuit in each cable.

2.2. Logic failure effect block diagrams

2.2.1. Start-up and initialisation.

Start-up and initialisation includes partial start-up of one node while the rest of the system is in normal operation. Total restart of all nodes must also be handled, as black-up may bring down the entire system.

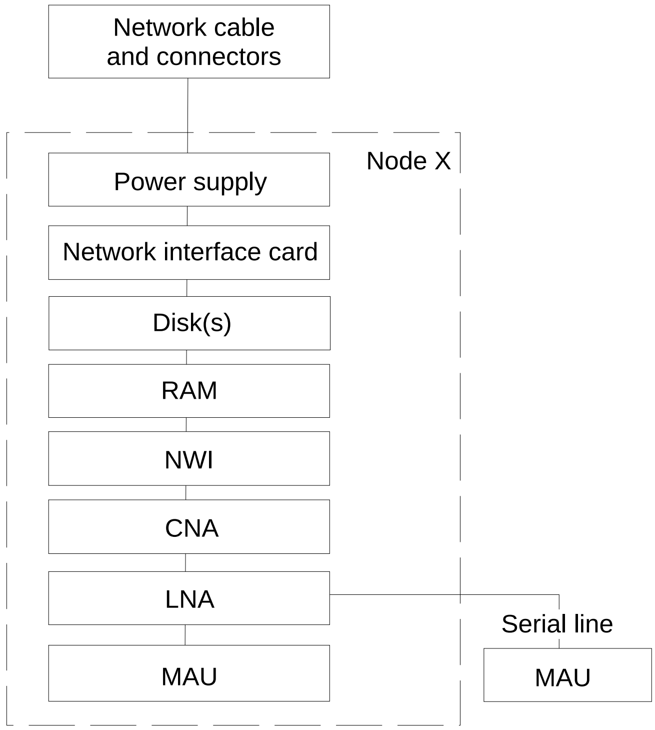

Figure 2.2.1. Start-up and initialisation.

2.2.2. Normal operation

Communication between two MiTS application units (MAUs) is the prime objective for the network system. For normal operation, the CNA is not part of the diagram. As far as this module have no effect on the rest of the system irrespective of failure mode, this module may not be considered.

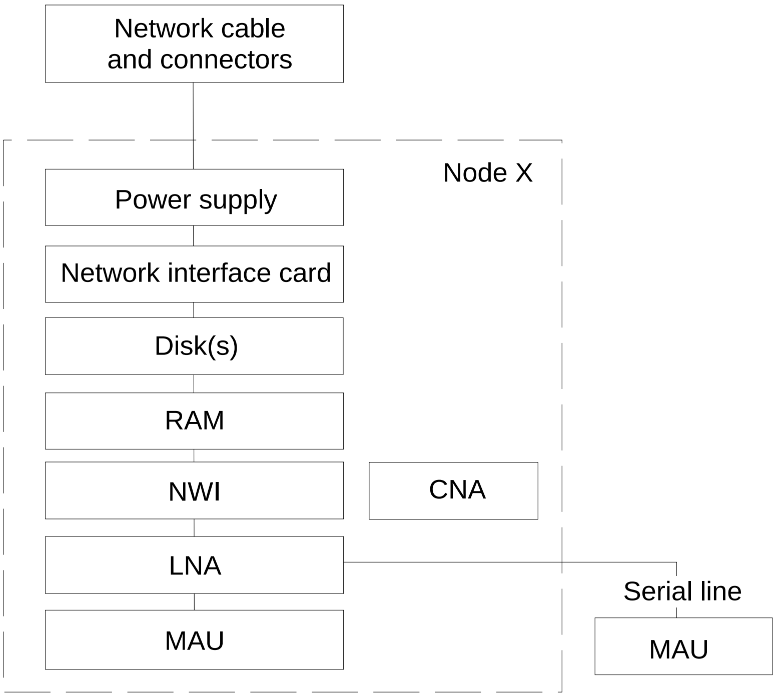

Figure 2.2.2. Normal operation.

2.3. Non-redundant network

All components as listed in table 1.4.1 are assigned typical failure modes for the various operation conditions. The failure modes are basically derived from the general list given in 1.3.

Result:

	Safe	Marginal	Severe	Critical
High	5	4		
Medium	7	10	1	2
Low	7	12		
Low-low	3	3		2

Table 2.3.1 Consequence versus probability

Case	Operation	Component	Failure mode	Possible failure cause	Detection	Local effect	Overall effect	Prob.	Cons.	Remark
2.3.1.	All operations	Network cable	No data transfer possible	Open circuit (wire breakage or connector out) due to vibration, external work (e.g. welding) or Short circuit due to flooding, pinched cable, etc.	Not in MiTS *	Node isolated	System has no communication	Medium	Critical	*) Each node reports comms error, but cause is not reported
2.3.2.	Start-up and normal operation	Network cable	Loss of part of data or noise generated in cable	Jitter due to vibration on loose contacts or nearly broken cable or spurious signals due to EMI	Not in MiTS	Lower available bandwidth. Slow operation ?	Lower available bandwidth. Slow operation ?	Medium	Marg*	*) Depends on severity of operation
2.3.3.	High load condition	Network cable	Loss of part of data or noise generated in cable	Jitter due to vibration on loose contacts or nearly broken cable or spurious signals due to EMI	Not in MiTS	Lower available bandwidth. Slow operation ?	Lower available bandwidth. Slow operation ?	Medium	Severe*	*) Depends on severity of problem
2.3.4.	All operations	Power supply	Not working	Black-out (no UPS)	Not in MiTS	No start	Node(s) lost	Medium	Critical	
2.3.5.	All operations	Power supply	Not working	UPS failure	Not in MiTS	No start	Node(s) lost	Low	Marg	
2.3.6.	All operations	Network interface card	Not working	PCB failure	Not in MiTS	Other nodes lost	Node lost	Low	Marg	
2.3.7.	All operations	Network interface card	Blocking network	Unscheduled transmission due to PCB error	Not in MiTS	Other nodes lost	Other nodes lost	Low-Low	Critical	
2.3.8.	All operations	Network interface card	Clamping network	Short circuit due to vibration	Not in MiTS	Other nodes lost	Other nodes lost	Low-Low	Critical	

Case	**Operation**	**Component**	**Failure mode**	**Possible failure cause**	**Detection**	**Local effect**	**Overall effect**	**Prob.**	**Cons.**	**Remark**
2.3.9.	All operations	Disk(s)	No contact	Disk crash	Not in MiTS	Not working	Node lost	Low	Marg	
2.3.10.	All operations	Disk(s)	Partial unavailability	Bad sector	Not in MiTS	Not working	Node lost	Medium	Marg	
2.3.11.	All operations	Disk(s)	No write access	Disk full	Not in MiTS	Application may not start/may crash	Node lost	Medium	Marg	
2.3.12.	All operations	RAM	Single bit error	RAM failure	Not in MiTS	Node lost and dead	Node lost	Medium	Marg	
2.3.13.	All operations	RAM	Block bit error	RAM or RAM controller failure	Not in MiTS	Node lost and dead	Node lost	Low	Marg	
2.3.14.	All operations	NWI	Not working	NWI not starting or socket not available	Comms-error in MiTS	Other nodes lost	Node lost	Low	Marg	
2.3.15.	All operations	NWI	Not working (dead node)	LNA, CNA or MAU overwriting kernel due to writing to zero-pointer	Segment violation error and crash in application most likely	Crash probably	Node lost	Low	Marg	Will not happen on memory-managed system
2.3.16.	Start-up and normal operation	NWI	Missed acknowledge	Jitter on cable, EMI	Not in MiTS	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Safe	

Case	**Operation**	**Component**	**Failure mode**	**Possible failure cause**	**Detection**	**Local effect**	**Overall effect**	**Prob.**	**Cons.**	**Remark**
2.3.17.	Start-up and normal operation	NWI	Loss of data	Missed packet due to jitter or EMI on cable	Not in MiTS	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Safe	
2.3.18.	Start-up and normal operation	NWI	Received garbage	Received bad packet (bit failure or part of packet) due to jitter or EMI on cable	Not in MiTS	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Safe	
2.3.19.	All operations	NWI	Sending garbage	Data interpretation error due to NWI software error or Sending bad packet (bit failure or part of packet) due to NWI, LNA, CNA or MAU software error or termination during transmission	On receiver end	None	Receiver will close jabbing node	Low	Marg	Pathological cases can be imagined (p=low-low)
2.3.20.	High load condition	NWI	Missed acknowledge	Jitter on cable, EMI	Not in MiTS	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Marg	Severity depends on severity of problem. Retransmissions will use bandwidth.
2.3.21.	High load condition	NWI	Loss of data	Missed packet due to jitter or EMI on cable	Not in MiTS	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Marg	Severity depends on severity of problem. Retransmissions will use bandwidth.
2.3.22.	High load condition	NWI	Received garbage	Received bad packet (bit failure or part of packet) due to jitter or EMI on cable	Not in MiTS	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Marg	Severity depends on severity of problem. Retransmissions will use bandwidth.

Case	**Operation**	**Component**	**Failure mode**	**Possible failure cause**	**Detection**	**Local effect**	**Overall effect**	**Prob.**	**Cons.**	**Remark**
2.3.23.	All operations	CNA	Erroneous operation or not working	CNA not starting or socket not available or Overwriting data or program area, e.g. configuration data due to inadvertent writing to erroneous pointer in CNA, LNA or MAU or Overwriting stack, data or program area due to too short string buffer or Processing, no action due to endless loop or Division by zero	In CNA & wrapper	Node isolated	Node isolated	Medium	Marg	
2.3.24.	All operations	CNA	Data missing	Missed packet due to jitter on cable, EMI or NWI software error	Not in MiTS	None	None	High	Safe	
2.3.25.	All operations	CNA	Receiving garbage	Received bad packet (wrong parameter or part of packet) due to remote CNA/LNA software error	Error message on CNA console	None	None	Medium	Safe	Pathological cases may be imagined (prob.=low, cons.=safe)
2.3.26.	All operations	CNA	Sending garbage	Sending bad packet (wrong parameter or part of packet) due to CNA software error or termination during transmission or Data interpretation error due to CNA software error	Error message on CNA console	None	None	Medium	Safe	May load network and cause problems at high loads.
2.3.27.	Start-up	CNA	Erroneous operation or not working	Erroneous input data due to bad manual input or packets with bad content	Not detected	Node isolated	Node isolated	High	Marg	Problem detected by not achieving connection ?
2.3.28.	Start-up	CNA	Erroneous operation or not working	Bad sequence due to programming error or race conditions	Not detected?	Node isolated	Node isolated	Low	Marg	Problem detected by not achieving connection ?

Case	**Operation**	**Component**	**Failure mode**	**Possible failure cause**	**Detection**	**Local effect**	**Overall effect**	**Prob.**	**Cons.**	**Remark**
2.3.29.	Start-up	CNA	Erroneous operation or not working	Out of buffer space due to too small buffers and no way to stop filling them up.	Close CNA-LNA connection	Node isolated	Node isolated	Medium	Marg	
2.3.30.	All operations	CNA	Request from unauthorised MAU	Hacking	Not detected	None	No significant effect	Low	Safe	
2.3.31.	Normal operation and High load condition	CNA	Not working	CNA not starting or socket not available or Overwriting data or program area, e.g. configuration data due to inadvertent writing to erroneous pointer in CNA, LNA or MAU or Overwriting stack, data or program area due to too short string buffer or Processing, no action due to endless loop or Division by zero	In LNA and/or wrapper	No new MAUs can make global connection	No new MAUs can make connection to node	Medium	Marg	
2.3.32.	Normal operation and High load condition	CNA	Erroneous operation or not working	Erroneous input data due to bad manual input or packets with bad content	Not detected	No new MAUs	No new connections to new MAUs on node	High	Marg	
2.3.33.	Normal operation and High load condition	CNA	Erroneous operation or not working	Bad sequence due to programming error or race conditions	Not detected	No new MAUs	No new connections to new MAUs on node	Low	Marg	
2.3.34.	Normal operation and High load condition	CNA	Erroneous operation or not working	Out of buffer space due to too small buffers and no way to stop filling them up.	LNA closed CNA-connection	No new MAUs	No new connections to new MAUs on node	Medium	Marg	

Case	**Operation**	**Component**	**Failure mode**	**Possible failure cause**	**Detection**	**Local effect**	**Overall effect**	**Prob.**	**Cons.**	**Remark**
2.3.35.	All operations	LNA	Request from unauthorised MAU	Hacking	No detection	None	None	Medium	Safe	
2.3.36.	Start-up	LNA	Not working	CNA not starting or socket not available	Warning at LNA console	No external connection established	Node isolated	Medium	Marg	
2.3.37.	Start-up and normal operation	LNA	Data missing	Missed packet due to jitter on cable, EMI or NWI software error	Not currently	None	None	Low	Safe	
2.3.38.	All operations	LNA	Receiving garbage	Received bad packet (wrong parameter or part of packet) due to remote CNA/LNA software error	Warning at console	Discarded, none	None	Low	Safe	
2.3.39.	All operations	LNA	Sending garbage	Sending bad packet (wrong parameter or part of packet) due to LNA software error or termination during transmission or Data interpretation error due to LNA software error	On remote LNA	None	Discarded, none	Lox	Safe	
2.3.40.	All operations	LNA	Erroneous operation or not working	Overwriting data or program area, e.g. configuration data due to inadvertent writing to erroneous pointer in CNA, LNA or MAU or Overwriting stack, data or program area due to too short string buffer or Division by zero	LNA stops	No MAU can start	No function on this node	Low	Marg	

Case	Operation	Component	Failure mode	Possible failure cause	Detection	Local effect	Overall effect	Prob.	Cons.	Remark
2.3.41.	All operations	LNA	Erroneous operation or not working	Processing, no action due to endless loop or Bad sequence due to programming error or race conditions or Erroneous input data due to bad manual input or packets with bad content	By MAU/CNA	No MAU can start	No function on this node	Low	Marg	
2.3.42.	Start-up and normal operation	LNA	Erroneous operation or not working	Out of buffer space due to too small buffers and no way to stop filling them up.	Close MAU or remote LNA	MAU/connections removed and then re-established	MAU/connections removed and then re-established	Medium	Safe	
2.3.43.	Normal operation and High load condition	LNA	Not working	CNA not starting or socket not available	On LNA console	No new connections	No new connections to new MAUs on node	Medium	Marg	
2.3.44.	High load condition	LNA	Data missing	Missed packet due to jitter on cable, EMI or NWI software error	No detection	None	None	Low	Marg*	*) Effect may depend on load and severity of problem
2.3.45.	High load condition	LNA	Erroneous operation or not working	Out of buffer space due to too small buffers and no way to stop filling them up.	Warnings + disconnect	Disconnect offending comms-line	Disconnect offending comms-line	High	Marg	
2.3.46.	All operations	MAU	Not working	CNA not starting or socket not available	LNA gives warning	No external connect	No connect with node	Medium	Safe	
2.3.47.	All operations	MAU	Data missing	Missed packet due to jitter on cable, EMI or NWI software error	Not detected	None	None	Low	Safe	
2.3.48.	All operations	MAU	Receiving garbage	Received bad packet (wrong parameter or part of packet) due to remote CNA/LNA software error	Warning	None	None	Low	Safe	Pathological cases may be envisaged

Case	Operation	Component	Failure mode	Possible failure cause	Detection	Local effect	Overall effect	Prob.	Cons.	Remark
2.3.49.	All operations	MAU	Sending garbage	Sending bad packet (wrong parameter or part of packet) due to LNA software error or termination during transmission or Data interpretation error due to LNA software error	Warning on LNA	Connection closed by LNA	MAU lost temporarily	Low	Safe	
2.3.50.	All operations	MAU	Erroneous operation or not working	Overwriting data or program area, e.g. configuration data due to inadvertent writing to erroneous pointer in CNA, LNA or MAU or Overwriting stack, data or program area due to too short string buffer	Warning on LNA	MAU down	MAU down temporarily	High	Safe	
2.3.51.	All operations	MAU	Not working	Processing, no action due to endless loop or Division by zero	LNA checks it	MAU down	MAU down	High	Safe	
2.3.52.	All operations	MAU	Erroneous operation or not working	Erroneous input data due to bad manual input or packets with bad content or Bad sequence due to programming error or race conditions	Not detected	Maloperation	Bad data ?	High	Safe	
2.3.53.	All operations	MAU	Erroneous operation or not working	Out of buffer space due to too small buffers and no way to stop filling them up.	In MAU	Close LNA	MAU down temporarily	Medium	Safe	Situation more probable for high load condition
2.3.54.	All operations	MAU	Request from unauthorised MAU	Hacking	In LNA	None if password is used	None	Medium	Safe	Require use of password

Case	Operation	Component	Failure mode	Possible failure cause	Detection	Local effect	Overall effect	Prob.	Cons.	Remark
2.3.55.	All operations	Serial lines	No data transfer possible	Open circuit (wire breakage or connector out) due to vibration, external work (e.g. welding) or Short circuit due to flooding, pinched cable, etc.	Time-out in MAU	No connection, may "jam" LNA	Node lost	High	Marg	Consequences are more important/obvious in high load conditions
2.3.56.	All operations	Serial lines	Loss of part of data or noise generated in cable	Jitter due to vibration on loose contacts or nearly broken cable or spurious signals due to EMI	Statistics in comlib	Lower speed	None	High	Safe	Consequences are more important/obvious in high load conditions

2.4. Redundant network

The redundancy is only for the network cable and the cable connectors, and is introduced to avoid a situation where all node looses the communication capabilities upon a failure on the network cable (especially short circuit and broken cable). The redundancy of the network interface card in each node is of minor advantage, and might be logically treated as on unit. As the hardware redundancy is present, this is shown. Redundancy for an application running on a node must be arranged running the same application on two separate nodes.

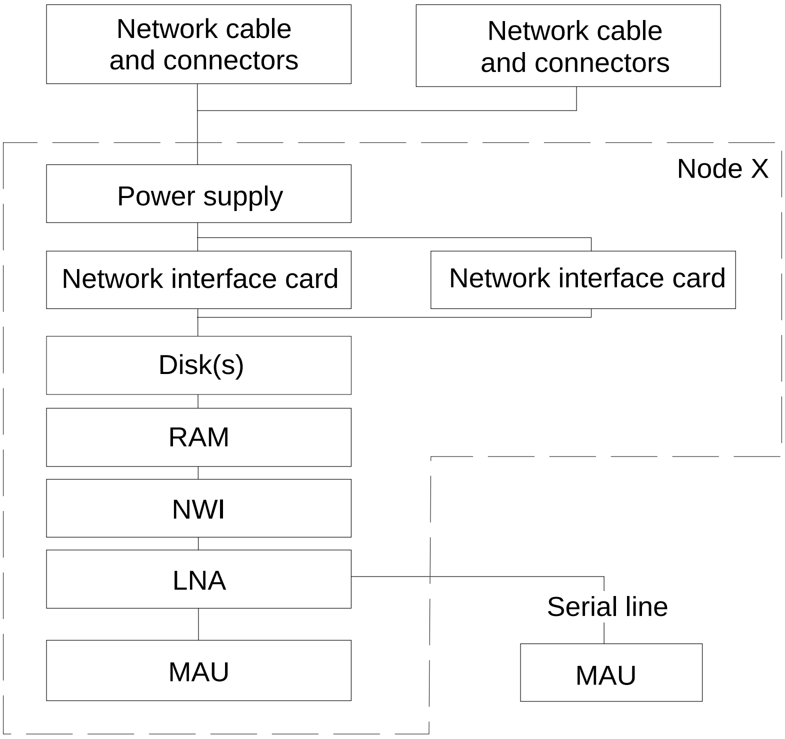

Figure 2.2.3 Communication on redundant network.

The table in the analysis contain the components that have any effected one the redundancy concept. The remaining components are covered in 2.3.

Result:

	Safe	Marginal	Severe	Critical
High				
Medium	2			
Low	3	3	1	
Low-low	3			

Table 2.4.1 Consequence versus probability

Case	**Operation**	**Component**	**Failure mode**	**Possible failure cause**	**Detection**	**Local effect**	**Overall effect**	**Prob.**	**Cons.**	**Remark**
2.4.1.	All operations	Network cable	No data transfer possible	Open circuit (wire breakage or connector out) due to vibration, external work (e.g. welding) or Short circuit due to flooding, pinched cable, etc.	In comlib	None	None	Medium	Safe	
2.4.2.	All operations	Network cable	Loss of part of data or noise generated in cable	Jitter due to vibration on loose contacts or nearly broken cable or spurious signals due to EMI	In comlib	None	None	Medium	Safe	
2.4.3.	All operations	Network interface card	Not working	PCB failure	In comlib ?	None	None	Low	Safe	
2.4.4.	Start-up and normal operation	Network interface card	Blocking network	Unscheduled transmission due to PCB error	In comlib ?	None	None	Low	Safe	Loads network and generates interrupts
2.4.5.	All operations	Network interface card	Clamping network	Short circuit due to vibration	In comlib ?	None	None	Low	Safe	
2.4.6.	High load condition	Network interface card	Blocking network	Unscheduled transmission due to PCB error	In comlib ?	None	None ?	Low	Marg to Severe	May cause high load on defect network
2.4.7.	All operations	NWI	Not working	NWI not starting or socket not available	Comms-error in MiTS	Other nodes lost	Node lost	Low	Marg	
2.4.8.	All operations	NWI	Not working (dead node)	LNA, CNA or MAU overwriting kernel due to writing to zero-pointer	Segment violation error and crash in application most likely	Crash probably	Node lost	Low	Marg	Will not happen on memory-managed system

Case	**Operation**	**Component**	**Failure mode**	**Possible failure cause**	**Detection**	**Local effect**	**Overall effect**	**Prob.**	**Cons.**	**Remark**
2.4.9.	All operations	NWI	Missed acknowledge	Jitter on cable, EMI	Better detection than for single network	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Safe Lower than for single network	Less critical, may be detected
2.4.10.	All operations	NWI	Loss of data	Missed packet due to jitter or EMI on cable	Better detection than for single network	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Safe Lower than for single network	Less critical, may be detected
2.4.11.	All operations	NWI	Received garbage	Received bad packet (bit failure or part of packet) due to jitter or EMI on cable	Better detection than for single network	TCP/IP will detect problem and correct it (p=0.999... 32+16 bit CRC) Slight delay	Slight delay	Low-low	Safe Lower than for single network	Less critical, may be detected
2.4.12.	All operations	NWI	Sending garbage	Data interpretation error due to NWI software error or Sending bad packet (bit failure or part of packet) due to NWI, LNA, CNA or MAU software error or termination during transmission	On receiver end	None	Receiver will close jabbing node	Low	Marg	Pathological cases can be imagined (p=low-low)

3. Findings and recommendations

3.1. General

The analysis is limited to the communication system itself, and is not concerned with the applications. When the results are assessed, it is important to have this in mind as findings classified as safe or marginal from the communication system point of view may be critical from an application point of view.

The consequence categories are selected as defined in 2.1.2 to give an indication of how failures propagates throughout the system. A general principle is that a single failure in the communication system should not spread and affect other parts of the system.

The results given in tables 2.3.1 and 2.4.1 show a good separation between nodes in the network. Most critical findings are related to failures for the cable in a single network. By introducing redundancy in the cabling, the consequence of these failure modes are reduced to an acceptable level. This result is as expected.

The difference between start-up, normal operation and high load conditions are found to be small. The reason for this is that MiTS basically supplies a network topology to the application programs. Internal errors that cause failures in the topology will generally have the same consequences regardless of load on the network. The exception is failures directly caused or directly causing traffic on the network, e.g., erroneous messages received or transmitted. These will get a higher probability and, usually, more severe consequences at higher loads.

3.2. Critical findings (CF)

2.3.1: Network cable failure.
As stated in 2.1.3 regarding common cause failures, the consequence of this failure is reduced down to an acceptable level when introducing redundancy for the cabling.

2.3.4: All nodes in the system supplied from the same power source.
As found in 2.3.5. and stated in 2.1.3, the consequence of this failure is reduced down to an acceptable level when installing of some sort of uninterruptible power supply.

2.3.7 and 2.3.8: Network interface card failure.
As for 2.3.1, the consequence of this failure is reduced down to an acceptable level when introducing redundancy.

3.3. Engineering comments (EC)

Generally, a wrapper task that keep track of the different components on a node (LNA, CNA, MAUs) must run. If a task disappears (crashes), it must be restarted. Additionally, a watchdog must trap crash of several programs (including the wrapper), and be able to do a full restart. This will make sure normal failures (statistical failures that crashes tasks) will be handled efficiently.

The three-level (administrative, system, instrument) system architecture should be strongly encouraged. It will make sure that the wrapper mechanism on the system level can be used without interrupting vital functions on the instrument level. It will also reduce the possibility of problems on the administrative level, e.g., ‘‘hacking” from propagating down to control levels.

The CNA should possibly check that there is traffic on the network. This may make it possible for a node to detect that it is isolated from the rest of the network.

A mechanism for logging of system error messages from LNA, CNA and MAUs is required. The messages should be stored and analysed if possible.

The CNA broadcast mechanisms should be examined to make sure it is not loading down the network in periods with high load.

When one of the networks in a dual network system have problems with excessive unintentional traffic, this network should possibly be closed down until the problem is corrected or order to start it is specifically given.

2.3.27.-33. and other: CNA failures not directly detected.
The MiTS communication library should have better facilities for detection of failures and transportation of the events to a higher level. The mechanisms for detection of communication problems are not good enough.

2.3.55. Open serial line.
RS232 serial line may cause a problems for computers having open lines. This must be considered in the construction phase. The serial line library should possibly close down bad serial line connections.

3.4. Areas requiring further investigation (FI)

MiTS is not yet tested for high load systems. The software and possibly the protocol may require changes to support such systems. ‘‘High load” should be defined.

MiTS may have to coexist with applications that require a substantial amount of network bandwidth, e.g., ECDIS charts transferred on the network. Consequences and guidelines for such situations should be developed.

General error reporting needs to be described in the companion standard (see also Section 3.3).